Finite Fields and Their Applications **6,** 294–301 (2000)
doi.10.1006/ffta.2000.0280, available online at http://www.idealibrary.com on IDEAL®

Linear $(q+1)$-fold Blocking Sets in $PG(2, q^4)$

Simeon Ball, Aart Blokhuis, and Michel Lavrauw

Technische Universiteit Eindhoven, Postbox 513, 5600 MB Eindhoven, The Netherlands

Communicated by James W. P. Hirschfeld

Received December 21, 1998; revised September 7, 1999; published online August 19, 2000

A $(q+1)$-fold blocking set of size $(q+1)(q^4+q^2+1)$ in $PG(2, q^4)$ which is not the union of $q+1$ disjoint Baer subplanes, is constructed © 2000 Academic Press

1. INTRODUCTION

Let $PG(2, q)$ and $AG(2, q)$, where $q = p^h$ and p is prime, be the Desarguesian projective and affine planes over $GF(q)$, the finite field of order q. An *s-fold blocking set* B in $PG(2, q)$ is a set of points such that every line of $PG(2, q)$ intersects B in at least s points. A 1-fold blocking set is simply called a *blocking set*. If a blocking set contains a line of $PG(2, q)$, then it is called *trivial*. A blocking set is said to be *minimal* or *irreducible* if it contains no proper subset which also forms a blocking set. For a survey on blocking sets, see Blokhuis [4]. Less is known about s-fold blocking sets, where $s > 1$. If the s-fold blocking set B in $PG(2, q)$ contains a line ℓ, then $B\backslash\ell$ is an $(s-1)$-fold blocking set in $AG(2, q) = PG(2, q)\backslash\ell$. The result from [2] gives the following:

Let B be an s-fold blocking set in $PG(2, q)$ that contains a line and let e be maximal such that $p^e|(s-1)$; then $|B| \geq (s+1)q - p^e + 1$.

This covers previous results by Bruen [7, 8], who proved the general bound $(s+1)(q-1)+1$, and Blokhuis [5], who proved $(s+1)q$ in the case $(p, s-1) = 1$.

If the s-fold-blocking set does not contain a line, then Hirschfeld [10, Theorem 13.31] states that it has at least $sq + \sqrt{sq} + 1$ points. A *Baer subplane* of a projective plane of order q is a subplane of order $\sqrt{q}$. The strongest result concerning s-fold blocking sets in $PG(2, q)$ not containing a line is a result of Blokhuis *et al.* [6]:

1071-5797/00 $35.00

Let B be an s-fold blocking set in $PG(2, q)$ of size $s(q+1)+c$. Let $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$.

1. *If $q = p^{2d+1}$ and $s < q/2 - c_p q^{2/3}/2$ then $c \geq c_p q^{2/3}$.*

2. *If $4 < q$ is a square, $s \leq q^{1/4}/2$, and $c < c_p q^{2/3}$, then $c \geq s\sqrt{q}$ and B contains the union of s disjoint Baer subplanes.*

3. *If $q = p^2$ and $s < q^{1/4}/2$ and $c < p\lceil 1/4 + \sqrt{(p+1)/2}\,\rceil$, then $c \geq s\sqrt{q}$ and B contains the union of s disjoint Baer subplanes.*

This result is proved using lacunary polynomials. It is clear that the union of s disjoint Baer subplanes in $PG(2, q)$, where q is a square, is an s-fold blocking set. A line intersects this set in either s or $\sqrt{q}+s$ points. The result stated above means that an s-fold blocking set of size $s(q+1)+c$, where c is a constant, necessarily contains the union of s disjoint Baer subplanes if s and c are small enough ($s \leq q^{1/6}$). The result we present here shows that this bound is quite good. We construct s-fold blocking sets of size $s(q+\sqrt{q}+1)$ in $PG(2, q)$, with $s = q^{1/4}+1$, which are not the union of s disjoint Baer subplanes.

2. THE REPRESENTATIONS

In the following we will use representations of projective spaces used in [1, 3].

The points of $PG(2, q)$ are the 1-dimensional subspaces of $GF(q^3)$, considered as a 3-dimensional vector space over $GF(q)$. Such a subspace has an equation that is $GF(q)$-linear of the form $P' = 0$, with

$$P' := x^q - \gamma x,$$

where $\gamma \in GF(q^3)$. So a point of $PG(2, q)$ is in fact a set $\{x \in GF(q^3) | x^q - \gamma x = 0\}$. Since elements of this set are also solutions of

$$-P'^{q^2} + (x^{q^3} - x) - \gamma^{q^2} P'^q - \gamma^{q^2+q} P' = 0$$

$$\Updownarrow$$

$$(\gamma^{q^2+q+1} - 1)x = 0$$

and this is an equation of degree ≤ 1 in x, we necessarily have that $\gamma^{q^2+q+1} = 1$. So points of $PG(2, q)$ can be represented by polynomials of the form $x^q - \gamma x$ over $GF(q^3)$, where $\gamma \in GF(q^3)$ and $\gamma^{q^2+q+1} = 1$. Actually this is just a special case of the representation of $PG(n, q)$ in $GF(q^{n+1})$, where, by analogous arguments, points can be represented by polynomials of the form $x^q - \gamma x$ over $GF(q^{n+1})$, with $\gamma \in GF(q^{n+1})$ and $\gamma^{q^n+q^{n-1}+\cdots+1} = 1$.

Now consider $PG(3, q)$. Points are represented by a polynomial of the form $x^q - \gamma x$ over $GF(q^4)$, with $\gamma \in GF(q^4)$ and $\gamma^{q^3+q^2+q+1} = 1$. A line in $PG(3, q)$ is a 2-dimensional linear subspace of $GF(q^4)$ (or $GF(q)^4$), which has a polynomial equation of degree q^2. Since this equation has to be $GF(q)$-linear, it is of the form $W' = 0$, with

$$W' := x^{q^2} + \alpha x^q + \beta x,$$

where $\alpha, \beta \in GF(q^4)$. So a line of $PG(3, q)$ is in fact a set $\{x \in GF(q^4) | x^{q^2} + \alpha x^q + \beta x = 0\}$. Since elements of this set are also zeros of

$$\begin{aligned} W'^{q^2} - (x^{q^4} - x) - \alpha^{q^2} W'^q - (\beta^{q^2} - \alpha^{q^2+q}) W' \\ = (-\alpha^{q^2}\beta^q - \alpha\beta^{q^2} + \alpha^{q^2+q+1}) x^q + (\alpha^{q^2+q}\beta - \beta^{q^2+1} + 1)x \end{aligned}$$

and this is an equation of degree $\leq q$, both coefficients on the right-hand side must be identically zero. Manipulating these coefficients we get the conditions $\beta^{q^3+q^2+q+1} = 1$ and $\alpha^{q+1} = \beta^q - \beta^{q^2+q+1}$. Again this is just a special case of the representation of $PG(n, q)$ in $GF(q^{n+1})$, where a k-dimensional subspace can be represented by a polynomial of the form

$$x^{q^{k+1}} + \alpha_1 x^{q^k} + \alpha_2 x^{q^{k-1}} + \ \ldots \ + \alpha_k x,$$

for some $\alpha_1, \alpha_2, \ \ldots \ , \alpha_k \in GF(q^{n+1})$. For a survey on the use of polynomials of this type in finite geometries, see [1].

3. CONSTRUCTION

We work in the Desarguesian projective plane $PG(2, q^t)$. The points of $PG(2, q^t)$ are the one-dimensional subspaces of $V(3, q^t)$. If we consider $GF(q^t)$ as a t-dimensional vector space over $GF(q)$, then every vector in $V(3, q^t)$, with 3 coordinates, can be seen as a vector in $V(3t, q)$, with $3t$ coordinates, just by expanding the coordinates over the field $GF(q)$. In this way a one-dimensional subspace in $V(3, q^t)$ induces a t-dimensional subspace in $V(3t, q)$. So the points of $PG(2, q^t)$ induce t-dimensional subspaces in $V(3t, q)$. The lines of $PG(2, q^t)$, which are 2-dimensional subspaces of $V(3, q^t)$, induce $2t$-dimensional subspaces in $V(3t, q)$. The points of $PG(2, q^t)$, seen as $(t-1)$-dimensional subspaces in $PG(3t-1, q)$, form a normal spread S of $PG(3t-1, q)$; see [11]. A $(t-1)$-*spread* of $PG(n, q)$ is a set of $(t-1)$-dimensional pairwise disjoint subspaces which partition the points of the whole space. We refer to a $(t-1)$-spread simply as a spread. A spread S of $PG(n, q)$ is called *normal* if and only if the space generated by two spread elements is also partitioned by the spread elements of S. From this it follows that any subspace generated by

spread elements of a normal spread is partitioned by spread elements and every 1-spread of $PG(3, q)$ is an example of a normal spread. We abuse notation and use S for the spread in $PG(3t-1, q)$ as well as in $V(3t, q)$. If W is a subspace of $V(3t, q)$, then by $B(W)$ we mean the set of points of $PG(2, q^t)$, which correspond to the elements of S which have at least a one-dimensional intersection with W in $V(3t, q)$. Since lines of $PG(2, q^t)$ induce $2t$-dimensional subspaces in $V(3t, q)$, it is clear that every $(t+1)$-dimensional subspace in $V(3t, q)$ induces a blocking set in $PG(2, q^t)$; see [12]. Every $(t+2)$-dimensional subspace in $V(3t, q)$ also induces a blocking set in $PG(2, q^t)$. But it induces a $(q+1)$-fold blocking set in $PG(2, q^t)$ if this $(t+2)$-dimensional subspace intersects every spread element in at most a one-dimensional subspace. An s-fold blocking set constructed in this way, is called a *linear s-fold blocking set*. We will use the following notation. If W is a subspace of $V(3t, q)$, then we define

$$\tilde{W} = \bigcup_{P:(P\in S)\wedge(P\cap W\neq\{\mathbf{0}\})} \{\mathbf{v}\,|\,\mathbf{v}\in P\}.$$

So in fact, $\tilde{W}$ is the union of the vectors of the spread elements corresponding to the points of $B(W)$.

In the following we will give a construction of a linear $(q+1)$-fold blocking set in $PG(2, q^4)$. Let

$$W' := x^{q^6} + \alpha x^{q^3} + \beta x$$

and

$$P' := x^{q^4} - \gamma x,$$

with $\alpha,\ \beta,\ \gamma \in GF(q^{12})$, $\gamma^{q^8+q^4+1} = 1$, $\beta^{q^9+q^6+q^3+1} = 1$ and $\alpha^{q^3+1} = \beta^{q^3} - \beta^{q^6+q^3+1}$. By Section 2 it is clear that $W = \{x \in GF(q^{12}) \| W' = 0\}$ is a 6-dimensional subspace of $V(12, q)$ and the set $P = \{x \in GF(q^{12}) \| P' = 0\}$ is a 4-dimensional subspace of $V(12, q)$.

THEOREM 3.1. *There exist $\alpha,\ \beta \in GF(q^{12})$, for which the set $B(W)$ is a $(q+1)$-fold blocking set of size $(q+1)(q^4+q^2+1)$ in $PG(2, q^4)$ and is not the union of $q+1$ disjoint Baer subplanes.*

Proof. First we show that the dimension of the intersection of the subspaces W and P in $V(12, q)$ is less than or equal to one. Solutions of both $W' = 0$ and $P' = 0$ are also solutions of

$$\begin{aligned}\alpha^q\beta^{q^2}(\gamma^{q^3}(W' - P'^{q^2}) - \alpha((W' - P'^{q^2})^q - \alpha^q P')) \\ - \gamma^{q^3+q^2}(((W' - P'^{q^2})^q) - \alpha^q P')\gamma^{q^4} \\ - (\gamma^{q^3}(W' - P'^{q^2}) - \alpha((W' - P'^{q^2})^q - \alpha^q P'))^q) = 0.\end{aligned}$$

This is

$$(-\beta^{(q^2+q)}\alpha^{(q+1)} - \gamma^{(q^3+q^2+q)}\alpha^{(q^2+q)})x^q$$
$$+ (-\gamma\beta^{q^2}\alpha^{(2q+1)} + \gamma^{q^3}\beta^{(q^2+1)}\alpha^q - \gamma^{(q^4+q^3+q^2+1)}\alpha^q)x = 0,$$

which is an equation of degree q in x. If the coefficients are not identically zero, then this equation will have at most q solutions. This means that the 6-dimensional subspace W intersects every spread element P in at most one dimension. So we have to prove that there exist $\alpha, \beta \in GF(q^{12})$, for which these coefficients are not identically zero.

Suppose

$$-\beta^{(q^2+q)}\alpha^{(q+1)} - \gamma^{(q^3+q^2+q)}\alpha^{(q^2+q)} = 0 \tag{1}$$

and

$$-\gamma\beta^{q^2}\alpha^{(2q+1)} + \gamma^{q^3}\beta^{(q^2+1)}\alpha^q - \gamma^{(q^4+q^3+q^2+1)}\alpha^q = 0. \tag{2}$$

Equation (1) implies that $\gamma^{q^3+q^2+q} = -\beta^{q^2+q}\alpha^{1-q^2}$, assuming $\alpha \neq 0$. Substitution in (2) gives us

$$-\alpha^{q+1} + \alpha^{q(q^{10}-1)(q-1)}\beta^{q^2} + \alpha^{q-q^3}\beta^{q^3} = 0$$

or

$$-\alpha^{q^3+1} + \beta^{q^3} + \alpha^{q^{12}-q^{11}+q^3-q^2}\beta^{q^2} = 0.$$

Since $\alpha^{q^3+1} = \beta^{q^3} - \beta^{q^6+q^3+1}$, this is equivalent to

$$\beta^{q^7+q^4-q^3+q} = -\alpha^{q^4-q^3+q-1}$$

or, again using $\alpha^{q^3+1} = \beta^{q^3} - \beta^{q^6+q^3+1}$, to

$$\beta^{q^7+q^4-q^3+q} = -(\beta^{q^3+1} - \beta^{q^6+q^3+1})^{q-1}. \tag{3}$$

This results in an equation of degree less than $q^7 + q^4$. So there are less than $q^7 + q^4$ possibilities for $\beta \in GF(q^{12})$ such that both coefficients are zero. We can conclude that there exist $\alpha, \beta \in GF(q^{12})$, for which these coefficients are not identically zero, namely, where $\alpha \neq 0$ and β does not satisfy (3).

Let m_i denote the number of lines of $PG(2, q^4)$ that intersect $B(W)$ in i points. Since a line induces a $2t$-dimensional subspace in $V(12, q)$, it is obvious that $m_i = 0$, for all $i \notin \{q+1, q^2+q+1, q^3+q^2+q+1,$

$q^4+q^3+q^2+q+1,\ q^5+q^4+q^3+q^2+q+1\}$. If one of the last two intersection numbers occurs, this means that there is a line, seen in $V(12, q)$ as an 8-dimensional subspace, having a 5- or 6-dimensional intersection with W. In both cases this implies that there is an element of the normal spread S intersecting W in more than one dimension, which is impossible. So we have that $m_i = 0$, for all $i \notin \{q+1, q^2+q+1, q^3+q^2+q+1\}$. Let us put $l_2 = m_{q+1}$, $l_3 = m_{q^2+q+1}$, and $l_4 = m_{q^3+q^2+q+1}$. Then by counting lines, point–line pairs, and point–point–line triples we obtain a set of equations from which we can solve l_2, l_3, and l_4 and these imply $l_2 = p^8 - p^5 - p^3 - p^2 - p$, $l_3 = p^5 + p^4 + p^3 + p^2 + p + 1$, and $l_4 = 0$. This implies that the 8-dimensional subspace corresponding to a line of $PG(2, q^4)$ intersects W in a 2- or 3-dimensional subspace of $V(12, q)$.

Suppose now that the $(q+1)$-fold blocking set $B(W)$ is the union of $q+1$ disjoint Baer subplanes of $PG(2, q^4)$. Let $B(\mathscr{B})$ be one of the Baer sublines of these Baer subplanes and let L be the line of $PG(2, q^4)$ containing $B(\mathscr{B})$. Then the 8-dimensional subspace induced by L intersects W in a 3-dimensional subspace D and $B(\mathscr{B})$ induces a 4-dimensional subspace $\mathscr{B}$ of $V(12, q)$ contained in the 8-dimensional subspace corresponding to L, which intersects every element of the spread S in a zero or two-dimensional subspace of $V(12, q)$. (See Bose *et al.* [9, Sect. 3] for a representation of a Baer subplane in $PG(5, q)$, which is analogous to this.) We will prove that $\tilde{\mathscr{B}}$ cannot be contained in $\tilde{D}$. First we observe that $\mathscr{B}$ is in fact a 2-dimensional subspace over $GF(q^2)$, so

$$\mathscr{B} = \{\alpha\mathbf{u} + \beta\mathbf{v} \| \alpha, \beta \in GF(q^2)\};$$

while D is a 3-dimensional subspace over $GF(q)$, so

$$D = \{\lambda\mathbf{w} + \mu\mathbf{x} + \nu\mathbf{y} \| \lambda, \mu, \nu \in GF(q)\}.$$

From this it follows that

$$\tilde{\mathscr{B}} = \{a(\alpha\mathbf{u} + \beta\mathbf{v}) \| \alpha, \beta \in GF(q^2), a \in GF(q^4)\}$$

and

$$\tilde{D} = \{b(\lambda\mathbf{w} + \mu\mathbf{x} + \nu\mathbf{y}) \| \lambda, \mu, \nu \in GF(q), b \in GF(q^4)\}.$$

Now observe that $\langle B(\mathbf{u}), B(\mathbf{v})\rangle$ over $GF(q^4)$ is in fact the line L. So we can write $\mathbf{w}$, $\mathbf{x}$, and $\mathbf{y}$ as linear combinations of $\mathbf{u}$ and $\mathbf{v}$ over $GF(q^4)$. Without loss

of generality, we can write

$$\mathbf{w} = c_1 u$$

$$\mathbf{x} = c_2 \mathbf{v}$$

$$\mathbf{y} = c_3 \mathbf{u} + c_4 \mathbf{v},$$

with $c_1, c_2, c_3, c_4 \in GF(q^4)$. But if $\tilde{\mathscr{B}}$ is contained in $\tilde{D}$, then for all $a \in GF(q^4)$ and $\alpha, \beta \in GF(q^2)$ there exist $b \in GF(q^4)$ and $\lambda, \mu, \nu \in GF(q)$ such that

$$\begin{cases} a\alpha = b(\lambda c_1 + \nu c_3) \\ a\beta = b(\mu c_2 + \nu c_4), \end{cases}$$

which results in the equation

$$\frac{\lambda c_1 + \nu c_3}{\mu c_2 + \nu c_4} = \frac{\alpha}{\beta} \in GF(q^2) \cup \{\infty\}.$$

Let f be the map

$$f: GF(q) \times GF(q) \times GF(q) \to GF(q^4) \cup \{\infty\}$$

given by

$$f(\lambda, \mu, \nu) = \frac{\lambda c_1 + \nu c_3}{\mu c_2 + \nu c_4}.$$

Then the image $\mathscr{S}(f)$ of f must contain $GF(q^2)$. We remark that if $\mathscr{S}(f) = GF(q^4) \cup \{\infty\}$, then $\tilde{D}$ must be contained in $\tilde{\mathscr{B}}$, which is impossible. But if $f(\lambda, \mu, \nu) \in GF(q^2)$, then

$$\left(\frac{\lambda c_1 + \nu c_3}{\mu c_2 + \nu c_4}\right)^{q^2} = \frac{\lambda c_1 + \nu c_3}{\mu c_2 + \nu c_4},$$

which gives us the equation

$$(\lambda c_1 + \nu c_3)^{q^2}(\mu c_2 + \nu c_4) - (\mu c_2 + \nu c_4)^{q^2}(\lambda c_1 + \nu c_3) = 0.$$

Since $\lambda, \mu, \nu \in GF(q)$, this equation results in a quadratic equation in λ, μ, and ν. Triples $(\lambda, \mu, \nu) \in GF(q)^3$ can only give different values for f if they do not belong to the same 1-dimensional subspace of $GF(q)^3$, that is, if they represent different points in $PG(2, q)$. So the above equation will have at most $2q + 1$

different solutions, namely the points of a degenerate quadric in $PG(2, q)$. If $q > 2$ then $2q + 1 < q^2 + 1$ and if $q = 2$ the final part of the proof can quite easily be verified by considering the various possibilities for f. ■

REFERENCES

1. S. Ball, Polynomials in finite geometries, *in* "Surveys in Combinatorics 1999," (J. D. Lamb and D. A. Preece, Eds.), London Math. Soc. Lecture Note Series, Vol. 267, pp. 17–35, Cambridge Univ. Press, Cambridge, UK, 1999.
2. S. Ball, On nuclei and blocking sets in Desarguesian spaces, *J. Combin. Theory Ser. A* **85** (1999), 232–236.
3. S. Ball, A. Blokhuis, and C. M. O'Keefe, On unitals with many Baer sublines, *Des. Codes Cryptogr.* **17** (1999), 237–252.
4. A. Blokhuis, Blocking sets in Desarguesian planes, *in.* "Paul Erdös is Eighty, Vol. 2" (D. Miklós, V. T. Sós, and T. Szönyi, Eds.), *Bolyai Soc. Math. Stud.* **2** (1996), 133–155.
5. A. Blokhuis, On multiple nuclei and a conjecture of Lunelli and Sce, *Bull. Belg. Math. Soc. Simon Stevin* **1** (1994), 349–353.
6. A. Blokhuis, L. Storme, and T. Szönyi, Lacunary polynomials, multiple blocking sets and Baer subplanes, *J. London Math. Soc.* (2), **60** (1999), 321–332.
7. A. A. Bruen, Arcs and multiple blocking sets, *in* Symposia Mathematics, Vol. 28, 15–29, XXVIII, Academic Press, London/New York, 1986.
8. A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *J. Combin. Theory Ser. A* **60** (1992), 19–33.
9. R. C. Bose, J. W. Freeman, and D. G. Glynn, On the intersection of two Baer subplanes in a finite projective plane, *Utilitas Math.* **17** (1980), 65–77.
10. J. W. P. Hirschfeld, "Projective Geometries over Finite Fields," 2nd ed., Clarendon, Oxford, 1998.
11. G. Lunardon, Normal spreads, *Geom. Dedicata* **75** (1999), 245–261.
12. P. Polito and O. Polverino, On small blocking sets, *Combinatorica* **18** (1998), 133–137.